**УТВЕРЖДАЮ**

**Директор Муниципального казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг Солнечногорского муниципального района Московской области»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_М.В.Панфилова**

**«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2015г.**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Создание системы защиты персональных данных на автоматизированных рабочих местах**

1. **Цели проекта:**

* приведение в полное соответствие с нормами Федерального закона от 26 июля 2006 года № 152 ФЗ «О персональных данных» автоматизированных рабочих мест (далее АРМ) Муниципального казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг Солнечногорского муниципального района Московской области», на которых функционируют информационные системы персональных данных (далее ИСПДн);
* обеспечение защиты от несанкционированного доступа (далее НСД) к информации и базам данных, находящимся на АРМ Муниципального казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг Солнечногорского муниципального района Московской области»;
* обеспечение антивирусной защиты к информации и базам данных, находящимся на АРМ Муниципального казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг Солнечногорского муниципального района Московской области»;
* оценка соответствия объекта требованиям стандартов и других нормативных документов по безопасности информации, утвержденных (согласованных) ФСТЭК (Гостехкомиссией) России.

1. **Наименование и содержание работ:**

Выполнение комплекса работ по построению системы защиты информации:

* аудит объекта информатизации;
* доработка комплекта организационно-распорядительной документации;
* приобретение сертифицированных средств защиты информации;
* установка и настройка сертифицированных средств защиты информации;
* проведение аттестационных испытаний ИСПДн.

1. **Основание для выполнения работ:**

Работы должны проводиться в соответствии со следующими нормативными правовыми актами:

1. **Перечень и количество поставляемых программных и программно-аппаратных средств защиты информации, а также перечень и объем оказываемых услуг:**
   1. Перечень и количество поставляемых программных и программно-аппаратных средств защиты информации приведен в таблице 1.

Таблица 1 – Перечень и количество поставляемых программных и

* 1. Перечень и объем оказываемых услуг по установке и настройке программных и программно-аппаратных средств защиты информации,приведен в таблице 2.
  2. Перечень и объем оказываемых услуг по доработке комплекта организационно – распорядительной документации и проведению аттестационных испытаний.

Перечень документов, предоставляемый Заказчиком для доработки Исполнителем, приведен в Таблице 3.

1. **Место оказания услуг**

## Услуги должны быть оказаны по адресу: Московская обл., г. Солнечногорск, ул. Тельнова, д.3/2.

1. **Место поставки средств защиты информации**

Поставку средств защиты информации необходимо осуществить по адресу: Московская обл., г. Солнечногорск, ул. Тельнова, д.3/2.

1. **Требования к используемым технологиям.**

Построение системы защиты информации должно осуществляться на базе применения современных информационных технологий и обеспечивать:

* расширяемость и гибкость управления конфигурацией системы;
* надежность и отказоустойчивость аппаратных и программных средств системы.

Средства защиты должны быть совместимы с программными и аппаратными средствами автоматизированной обработки и защиты ПДн, используемыми заказчиком.

Архитектура СЗПДн должна быть открытой, масштабируемой и строиться по модульному принципу, каждый модуль должен обеспечивать свою часть функциональности решения задач в целом.

1. **Сроки поставки средств защиты и оказания услуг**
   1. В части поставки средств защиты информации - 10 (десять) рабочих дней с момента заключения муниципального контракта.
   2. В части оказания услуг – 15 (пятнадцать) рабочих дней с момента заключения муниципального контракта.
2. **Общие требования к лицензионному системному и прикладному программному обеспечению, средствам защиты информации, их качеству, техническим характеристикам и** **безопасности:**
   1. Требования к средству защиты информации от несанкционированного Secret Net 7 (сетевой режим работ).

Должно осуществлять***:***

* защиту серверов и рабочих станций от НСД;
* контроль входа пользователей в систему, в том числе и с использованием аппаратных средств защиты;
* разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;
* разграничение доступа пользователей к информации;
* контроль утечек информации;
* регистрацию событий безопасности и аудит.

Требования к операционной платформе и аппаратной части:

* + 32-битные операционные системы: MS Windows Server 2003 SP2, MS Windows Server 2003 R2 SP2, MS Windows Server 2008 SP2, MS Windows XP Professional SP3, MS Windows Vista SP2, MS Windows 7 SP1; MS Windows 8/8.1;
  + 64-битные операционные системы: MS Windows Server 2003 x64 Edition SP2, MS Windows Server 2003 R2 x64 Edition SP2, MS Windows Server 2008 x64 Edition SP2, MS Windows Server 2008 R2 x64 Edition SP1, MS Windows XP Professional x64 Edition SP2, MS Windows Vista x64 Edition SP2, MS Windows 7 x64 Edition SP1; MS Windows 8/8.1;Windows Server 2012/Server 2012 R2;
* Active Directory/ADAM/LDS (для применения СЗИ с централизованным управлением);
* наличие привода CD-ROM;
* в случае совместного применения средств доверенной загрузки - наличие свободного разъёма системной шины стандарта PCI версий 2.0, 2.1, 2.2, 2.3 с напряжением питания 5 В или 3,3 В, или свободный разъем PCI-Express.

Требования к функциональности:

* может функционировать совместно с аппаратными и программно-аппаратными средствами доверенной загрузки для обеспечения защиты компьютера от несанкционированной загрузки автоматизированной системы с внешних носителей;
* может функционировать совместно с персональными идентификаторами (для обеспечения усиленной аутентификации пользователей);
* поддерживать персональные идентификаторы iButton (при совместном использовании со средствами доверенной загрузки), eToken PRO, eToken PRO Java (в форм-факторах USB и смарт карт), Rutoken;
* должно обеспечивать автоматическую блокировку автоматизированной системы при изъятии персонального идентификатора пользователя;
* поддержка терминального режима работы пользователей для платформ Microsoft и Citrix, а так же при использовании бездисковых рабочих станций (“тонких клиентов”);
* контроль устройств:
* последовательные и параллельные порты;
* локальные устройства
* сменные, логические и оптические диски;
* USB – устройства,
* устройства PCMCI,
* устройства IEEE1394,
* устройства Secure Digital;
* контроль устройств подключаемых/отключаемых в процессе работы автоматизированной системы;
* контроль неизменности аппаратной конфигурации компьютера;
* управление подключениями (IrDA, WiFi, FireWire, Ethernet, Bluetooth);
* контроль вывода информации на отчуждаемые носители;
* теневое копирование отчуждаемой информации;
* разграничение доступа к принтерам;
* контроль буфера обмена Windows;
* создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера;
* должно обеспечивать автоматическую настройку механизмов защиты при добавлении в систему приложения, обрабатывающего конфиденциальную информацию;
* возможность выбора уровня конфиденциальности сессии для пользователя;
* разграничение доступа пользователей к конфиденциальным данным и приложениям;
* мандатное управление доступом, включая – к устройствам;
* контроль вывода конфиденциальных данных на печать, управление грифами конфиденциальности при печати конфиденциальных и секретных документов;
* контроль целостности файлов, каталогов, элементов системного реестра;
* возможность контроля целостности до загрузки операционной системы (при совместном применении со средствами доверенной загрузки);
* функциональный контроль ключевых компонентов системы;
* - автоматическое затирание данных на диске при удалении конфиденциальных файлов пользователем;
* регистрация событий безопасности в журнале безопасности;
* возможность автоматического оповещения по электронной почте о событиях несанкционированного доступа;
* возможность формирования отчетов по результатам аудита;
* реакции СЗИ при нарушении целостности:
* регистрацию события в журнале;
* блокировку компьютера;
* восстановление повреждённой/модифицированной информации;
* отклонение или принятие изменений;
* функциональный самоконтроль подсистем защиты.

Требования к централизованному управлению в доменной сети:

* централизованный мониторинг и оперативное управление рабочими станциями;
* централизованный сбор и хранение журналов безопасности, регистрация событий безопасности;
* аудит безопасности, формирования отчетов по результатам аудита;
* возможность создания централизованной политики безопасности по использованию отчуждаемых USB носителей информации;
* возможность создания централизованной политики замкнутой программной среды;
* возможность интеграции с политиками безопасности Active Directory;
* централизованное управление в сложной доменной сети (domain tree) должно функционировать по иерархическому принципу;
* должно обеспечивать создание доменов безопасности в территориально-распределенной сети, при этом предоставляется возможность делегирования административных полномочий по информационной безопасности;
* возможность создания отчетов по перечню установленного ПО, сведениям о ресурсах, объектах и параметрах защищаемого компьютера;

Требования по сертификации:

* должно быть сертифицировано на соответствие требованиям ФСТЭК России для применения в информационных системах персональных данных (ИСПДн) до класса К1 включительно;
* показатель защищенности от НСД (Гостехкомиссия России, 1999) не ниже 3-го класса защищенности. Классификация по уровню отсутствия НДВ (Гостехкомиссия России, 1999) – не ниже 2-го уровня контроля;
* может использоваться при создании автоматизированных систем до класса защищенности 1Б включительно.
  1. Требования к программно-аппаратному комплексу "Соболь". Версия 3.0. или эквивалент.

Должен осуществлять:

* идентификацию и аутентификацию пользователей;
* доверенную загрузку;
* контроль целостности программной среды;
* ведение журнала регистрации событий.

Требования к аппаратной части:

* Возможность исполнения АПМДЗ на платах PCI или PCI-Express;
* Формат платы: PCI Express;
* возможность работы со следующими идентификаторами iButton DS 1992, 1995 и 1996; iKey 2032; eToken Pro; Etoken PRO (Java); Rutoken S, Rutoken RF S; смарт-карты eToken PRO через USB-считыватель Athena ASEDrive IIIe USB V2\*.

Требования к функциональности:

* идентификация пользователей должна производиться по личному идентификатора, а аутентификацию во вводимому с клавиатуры паролю
* АПМДЗ должен иметь возможность контролировать целостность ОС :Windows Server 2003 (32 и 64 bit), Windows XP, Windows Vista(32 и 64 bit), Windows Server 2008(32 и 64 bit), Windows 7 (32 и 64 bit), АльтЛинукс СПТ6, Astra Linux Spesial Edition;
* наличие сторожевого таймера;
* контроль целостности реестра Windows\*;
* ведение системного журнала безопасности в энергонезависимой памяти АПМДЗ;
* контроль конфигурации\*;
* контроль журнала транзакций NTFS и EXT3;
* возможность программной инициализации АПМДЗ (без вскрытия системного блока);
* должна осуществляться блокировка загрузки ОC с внешних носителей (USB, CD-Rom и т.д.);
* поддержка файловых систем NTFS, FAT 16 и FAT 32, ext 2, ext 3, ufs.

Требования по сертификации:

* должен быть сертифицирован на соответствие требованиям ФСТЭК России «Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню не ниже 2-го и